VA'S INFORMATION SECURITY PROGRAM

TESTIMONY OF
THE HONORABLE RICHARD J. GRIFFIN
INSPECTOR GENERAL
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS

HOUSE COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

March 13, 2002

Mr. Chairman and Members of the Subcommittee, I am here today to report on our findings concerning the Department of Veterans Affairs (VA) Automated Information System (AIS) security program. Our work continues to identify serious Department-wide weaknesses in AIS security. As a result, we concluded in our audit of VA's Consolidated Financial Statements for Fiscal Years 2001 and 2000 that the Department must continue to designate information security as a material weakness area under the Federal Manager's Financial Integrity Act (FMFIA).

Since our April 4, 2001 testimony to this Subcommittee, we completed our first annual national audit of VA's information security program with a report issued on October 24, 2001. A second annual audit is currently in process. The audit has begun with a review of VBA's information security and in the weeks ahead will include the remainder of the Department. Our current audit work in VBA shows that significant information security vulnerabilities continue to place the Department at risk of:

- Denial of service attacks.

- Disruption of mission critical systems.

- Unauthorized access to and disclosure of data subject to Privacy Act protection and sensitive financial data.

In order to begin to effectively address its information security program weaknesses, we recommended in our October report that VA take the following actions:

- Establish centralized information security budgetary control for all information technology initiatives.

- Expedite actions to: (1) fill information security officer positions; (2) implement enterprise-wide intrusion detection, antivirus detection, and remediation plans; and (3) upgrade external electronic connections.

- Complete vulnerability assessments for all VA systems to address information security weaknesses exploited during our penetration testing.
- Direct Administration CIOs to: (1) address information system security vulnerabilities identified by the audit; (2) implement a VA-wide vulnerability assessment process; and, (3) enhance security awareness and highlight the need to assure compliance with existing VA information security policy, procedures, and controls.

- Assure that operation of all uncertified Independent Internet Gateways is discontinued.

- Establish minimum acceptable enterprise-wide security configuration standards involving desktop computers used in VA's automated systems, and require that Administration CIOs complete necessary upgrades/replacements.

- Centralize information security oversight and control over VA Central Office network operations.

- Eliminate physical security weaknesses identified by the audit at VA data centers and field facilities.

- Assure that VA's planned information security remediation actions address the areas of non-compliance with GISRA and OMB Circular A-130, Appendix III.

- Update VA's Critical Infrastructure Protection Plan to reflect current planned milestone dates for completing security initiatives and include measures to implement the GISRA requirements.

Much work remains to be done to implement necessary security enhancements to properly secure VA's systems and sensitive data. The Department's CIO (Assistant Secretary for Information and Technology), the individual Administrations, and other VA elements have responded positively to the audit findings and agreed to take various corrective actions. However, our current audit found that the Veterans Benefits Administration (VBA) did not complete some agreed to corrective actions at its Data Centers and Regional Offices. Our audit found that many of the information system security weaknesses reported in our 2001 audit remain unresolved, and additional security weaknesses were identified. We have advised VBA top management that this situation requires immediate corrective action to assure protection of critical Department electronic infrastructure resources and continuity of operations and delivery of services to the nation's veterans.

Our current audit work also shows that additional action is needed to prioritize completion of key security initiatives, establish timelines for completion, and secure necessary budget resources.

Key Department Security Remediation Actions Need To Be Prioritized And Completed In The Next Year

Our review of the Department's planning documents found that completion of necessary remediation actions has not been prioritized with timeline start and completion dates. We believe that this is a necessary step in the planning process to help assure that those most serious security weakness areas are targeted for completion first, based on the level of risk to Department operations and assets. Prioritization of the Department's security remediation actions is important to assure that resource expenditures are properly focused and provide the maximum opportunity to strengthen the Department-wide security posture in the near term (next 12 months). This is also important because our discussion with officials in the Department's Office of Cyber Security (OCS) indicated concern that budget resources may not be available to complete all necessary remediation actions.

Based on our results and discussion with officials in the OCS, we identified the following key security weakness areas that should be considered for priority completion in the next year. Some of these weakness areas require enforcement of existing Department policy and Governmental regulations and others require new hardware, software, and or contractor support to correct.

- **Intrusion Detection Systems (IDS)**
- **Infrastructure Protection**
- **Data Center Contingency Planning**
- **Certification and Accreditation of Systems**
- **Upgrade/Terminate External Connections**
- **Configuration Management**
- **Application Program/Operating System Change Controls**
- **Physical Access Controls (access to computer rooms)**

We believe that correction of these key information security weakness areas will provide the Department with the opportunity to better strengthen its national security posture in the short term and reduce the vulnerability of the Department's programs and sensitive data to potential destruction, manipulation, and inappropriate disclosure. Completion of these actions will also help the Department address existing information security control weaknesses that contribute to the designation of information security as a Department material weakness area under FMFIA. In response to our findings, the Department has identified these key information security weakness areas in its GISRA remediation action plan for priority corrective action in the next 12 months.

Annual Department Security Expenditure Requirements Are Significant

Once these security initiatives are prioritized for completion, necessary budget resources will need to be secured. We recognize that the Department faces a significant challenge to implement necessary security remediation actions that are estimated to require $804 million (Fiscal Years 2002-2006). This represents substantial budget resource expenditures above those levels funded in past years. In Fiscal Year (FY) 2001, about $17 million was expended for cyber security program initiatives in support of OCS efforts to strengthen the Department's national security posture. During FY 2002, about $21.4 million is budgeted for OCS directed security program initiatives. This level of funding support is significantly below the $93.2 million budget requirements identified in the Department's Cyber Security Capital Investment Proposal. In FY 2003, the level of projected security funding requirements increases to over $132 million. In addition to OCS directed security program expenditures, each of the Department Administration's budgets also includes security program expenditures that address various security initiatives. For FY 2002, these planned expenditures are significant and total an estimated $34.4 million.

During our current audit, we will be reviewing individual Administration security expenditures to assess the value of those expenditures in light of VA's national security priorities.

Conclusion

VA has been slow to implement a risk management framework to proactively identify information security related risks and implement corrective action. We evaluated VA compliance with requirements of GISRA and OMB Circular A-130, Appendix III. We found that VA has complied with provisions relating to organization, planning, and risk assessment, but additional effort is needed to effectively implement required agency wide security controls, monitoring, and assessment.

The Department has established a VA-wide security plan, policies, procedures, and guidelines as required by the Act. In addition, the Department has established performance measures for executive level managers in all Administrations. The establishment of performance measures for other managers is in process.

VA has not effectively implemented planned security measures and has not assured compliance with established policies, procedures, and control requirements. Based on the audit work completed and in process, VA is not in compliance with the GISRA requirements. To attain compliance with the Act, VA needs to:

- Improve information security awareness training for all VA employees.
- Fully implement the Critical Incident Response Capability.
- Assure that the Critical Infrastructure Protection Program is implemented and addresses GISRA requirements.
- Complete risk assessments of all VA systems.

The Department should also identify information security best practices both within and outside of VA that can be used to help implement the requirements of the Act. As an example, we found that one of VBA's data centers had established a hardened security screening process for all electronic information entering the facility. This process, which should be implemented system wide, limits access to VA systems, examines e-mail for malicious code, and prohibits access by unauthorized persons.

This concludes my testimony. I would be pleased to answer any questions that you and the members of the subcommittee may have.